PREMIER MINISTRE

Secrétariat général de la défense et de la sécurité nationale

Agence nationale de la sécurité des systèmes d'information

Rapport de certification ANSSI-CC-2017/55

NPCT6xx TPM 2.0

Hardware version FB5C85D and FB5C85E,
Firmware version 1.3.0.1, 1.3.1.0 and 1.3.2.8

Paris, le 25 septembre 2017

Le directeur général de l'agence nationale
de la sécurité des systèmes d'information

Guillaume POUPARD
[ORIGINAL SIGNE]

Avertissement

Ce rapport est destiné à fournir aux commanditaires un document leur permettant d'attester du niveau de sécurité offert par le produit dans les conditions d'utilisation ou d'exploitation définies dans ce rapport pour la version qui a été évaluée. Il est destiné également à fournir à l'acquéreur potentiel du produit les conditions dans lesquelles il pourra exploiter ou utiliser le produit de manière à se trouver dans les conditions d'utilisation pour lesquelles le produit a été évalué et certifié ; c'est pourquoi ce rapport de certification doit être lu conjointement aux guides d'utilisation et d'administration évalués ainsi qu'à la cible de sécurité du produit qui décrit les menaces, les hypothèses sur l'environnement et les conditions d'emploi présupposées afin que l'utilisateur puisse juger de l'adéquation du produit à son besoin en termes d'objectifs de sécurité.

La certification ne constitue pas en soi une recommandation du produit par l'agence nationale de la sécurité des systèmes d'information (ANSSI), et ne garantit pas que le produit certifié soit totalement exempt de vulnérabilités exploitables.

Toute correspondance relative à ce rapport doit être adressée au :

Secrétariat général de la défense et de la sécurité nationale
Agence nationale de la sécurité des systèmes d'information
Centre de certification
51, boulevard de la Tour Maubourg
75700 Paris cedex 07 SP

certification@ssi.gouv.fr

Référence du rapport de certification

ANSSI-CC-2017/55

Nom du produit

NPCT6xx TPM 2.0

Référence/version du produit

Hardware version FB5C85D and FB5C85E,
Firmware version 1.3.0.1, 1.3.1.0 and 1.3.2.8

Conformité à un profil de protection

[ANSSI-CC-PP-2015/07] PC Client Specific Trusted Platform Module,
Family 2.0, Level 0, Revision v1.16, Version 1.0

Critères d'évaluation et version

Critères Communs version 3.1 révision 4

Niveau d'évaluation

EAL 4 augmenté
ALC_DVS.2, ALC_FLR.1, AVA_VAN.4

Développeur(s)

Nuvoton Technology Israel Ltd.
8 Hasadnaot St, POB 3007, Herzlia B. 46130, Israël

Commanditaire

Nuvoton Technology Israel Ltd.
8 Hasadnaot St, POB 3007, Herzlia B. 46130, Israël

Centre d'évaluation

Serma Safety & Security
14 rue Galilée, CS 10055, 33615 Pessac Cedex, France

Accords de reconnaissance applicables

CCRA

SOG-IS

Ce certificat est reconnu au niveau EAL2 augmenté de FLR.1.

Préface

La certification

La certification de la sécurité offerte par les produits et les systèmes des technologies de l'information est régie par le décret 2002-535 du 18 avril 2002 modifié. Ce décret indique que :

- L'agence nationale de la sécurité des systèmes d'information élabore les **rapports de certification**. Ces rapports précisent les caractéristiques des objectifs de sécurité proposés. Ils peuvent comporter tout avertissement que ses rédacteurs estiment utile de mentionner pour des raisons de sécurité. Ils sont, au choix des commanditaires, communiqués ou non à des tiers ou rendus publics (article 7).
- Les **certificats** délivrés par le Premier ministre attestent que l'exemplaire des produits ou systèmes soumis à évaluation répond aux caractéristiques de sécurité spécifiées. Ils attestent également que les évaluations ont été conduites conformément aux règles et normes en vigueur, avec la compétence et l'impartialité requises (article 8).

Les procédures de certification sont disponibles sur le site Internet www.ssi.gouv.fr.

Table des matières

1. Le produit

1.1. Présentation du produit

Le produit évalué est « NPCT6xx TPM 2.0, Hardware version FB5C85D and FB5C85E, Firmware version 1.3.0.1, 1.3.1.0 and 1.3.2.8 » développé par *NUVOTON TECHNOLOGY ISRAEL LTD*.

Ce produit est destiné à garantir l'intégrité matérielle et logicielle des plateformes de confiance (serveurs, ordinateurs, etc.) conformément aux spécifications fonctionnelles TPM (*Trusted Platform Module*).

1.2. Description du produit

1.2.1. Introduction

La cible de sécurité [ST] définit le produit évalué, ses fonctionnalités de sécurité évaluées et son environnement d'exploitation.

Cette cible de sécurité est conforme au profil de protection [ANSSI-CC-PP-2015/07].

1.2.2. Services de sécurité

Les services de sécurité fournis par le produit sont principalement ceux décrits par le profil de protection [ANSSI-CC-PP-2015/07] :

- l'exécution des instructions TPM et l'implémentation de la machine d'état TPM ;
- l'authentification de l'entité propriétaire ;
- la gestion des registres de configuration (PCR[1]) ;
- la génération, l'exportation et l'importation de fichiers chiffrés (BLOB[2]) contenant des données du type : clés, valeurs de registres de configuration, etc. ;
- la configuration de sécurité ;
- la gestion de délégation et la gestion de la localité ;
- l'accès aux fonctions cryptographiques (RSA, AES, ECC, SHA1, SHA-256, HMAC, MGF1) ;
- le stockage de la paire de clés EK[3] ;
- la génération de clés et le stockage des clés (SRK[4]) ;
- la génération de nombres aléatoires ;
- la séquence de démarrage et l'auto-test ;
- la protection physique par un bouclier actif (*active shield*) ;
- un ensemble de détecteurs de sécurité (*glitch*, parité, etc.) ;
- la mise à jour du logiciel embarqué sur le produit.

[1] *Platform Configuration Register.*
[2] *Binary Large Object.*
[3] *Endorsement Key.*
[4] *Storage Root Key.*

1.2.3. Architecture

L'architecture matérielle du composant « NPCT6xx TPM 2.0, Hardware version FB5C85D and FB5C85E, Firmware version 1.3.0.1, 1.3.1.0 and 1.3.2.8 » est illustrée par la figure 1.

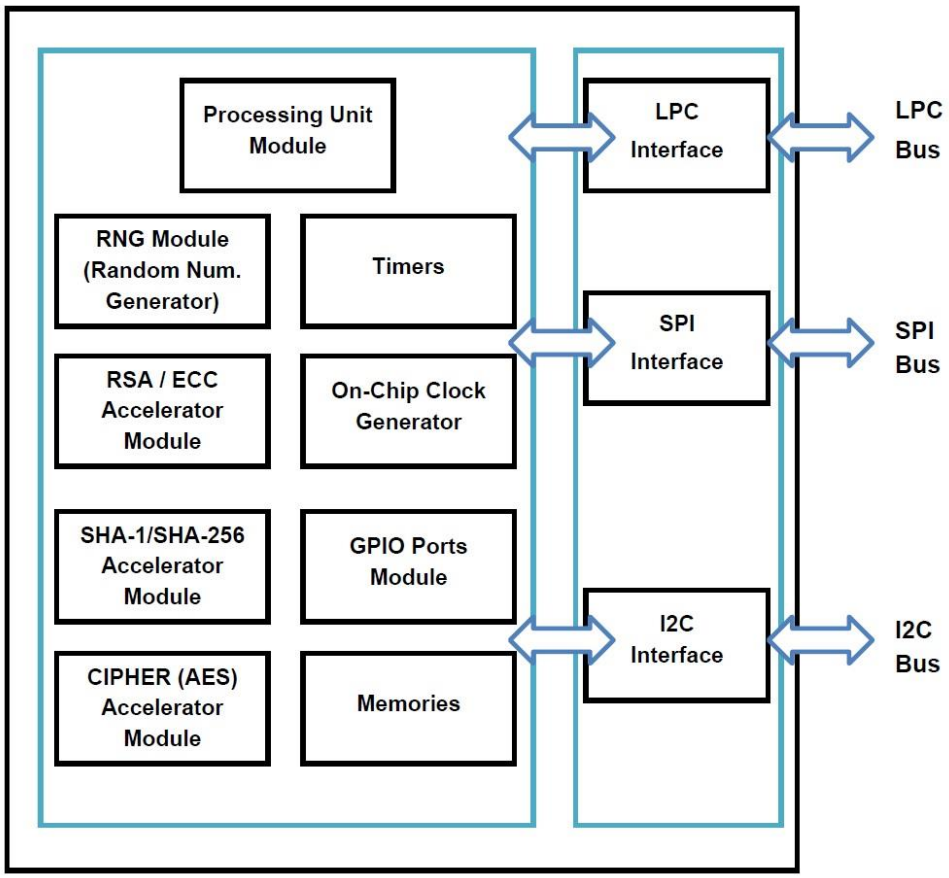


Figure 1. Architecture

Le composant est constitué des modules suivants :

- une unité centrale ;
- des unités d'interfaces GPIO[1], LPC[2], SPI[3], I2C[4] ;
- un générateur de nombres aléatoires ;
- des modules d'accélération cryptographique pour le support des calculs RSA/ECC, AES, SHA-1/SHA-256 ;
- des blocs mémoires de type ROM (44 Koctets), RAM (32 Koctets), cache (1 Koctets) et OTP[5] (128 octets) ;
- un bloc *Timers.*

[1] *General Purpose Input Output.*
[2] *Low Pin Count.*
[3] *SerialPeripheral Interface.*
[4] *Inter Integrated Circuit.*
[5] *One-Time Programmable.*

1.2.4. Identification du produit

Les éléments constitutifs du produit sont identifiés dans la liste de configuration [CONF].

La version certifiée de la TOE est identifiable par les éléments suivants (voir [GUIDES]) :

- la version matérielle « FB5C85 » est inscrite sur le composant ;
- la version logicielle est obtenue par la commande TPM_GetCapability qui, pour les tags TPM_PT_FIRMWARE_VERSION_1 et TPM_PT_FIRMWARE_VERSION_2 renvoie les données identifiant les versions *firmware* 1.3.0.1, 1.3.1.0 and 1.3.2.8.

1.2.5. Cycle de vie

Le cycle de vie du produit est décrit dans la cible de sécurité (voir [ST]).

Le produit a été développé et fabriqué sur les sites suivants :

NUVOTON TECHNOLOGY ISRAEL
Design Center Hasadnaot 8,
Hertzelia, Israël

NUVOTON TECHNOLOGY ISRAEL
Design Center2 Ataa'sia 8, Ramat Gavriel,
Migdal Haemek, Israël

TOPPAN PHOTOMASKS GERMANY
Mask Fab Germany
Rähnitzer Allee 9,
01109 Dresden, Allemagne

TSL WAFER FAB
Ramat Gavriel Industrial
Area, Migdal Haemek, Israël

TOWERJAZZ PANASONIC SEMICONDUCTOR CORPORATION (TPSCO)
271 Higashi-kaihotsu, Tonami City
Toyama, 939-1312, Japan

MATSUDA SANGYO CO. LTD
87-1 Negishi, Iruma city
Saitama, 358-0034, Japan

ASE GROUP CHUNG-LI
Assembly plants, 550, Chung-Hwa Road,
Section 1, Chung-Li, 320,
Taïwan, République de Chine

AMKOR TECHNOLOGY PHILIPPINES, INC.
Assembly plants, (ATP) - P1, KM 22 East
Service Road, Special Economic Zone,
Cupang, Muntinlupa City, 1702, Philippines

AMKOR TECHNOLOGY PHILIPPINES, INC.
Assembly plants, (ATP) - P3/P4, 119 North
Science Avenue, Special Economic
Processing Zone, Laguna Technopark,
Binan Laguna, 4024, Philippines

NTC WAFER TEST AND FINAL TEST PLANT NO. 4,
Creation Rd. III, Hsinchu Science Park,
Taïwan, République de Chine

1.2.6. Configuration évaluée

Le certificat porte sur le composant programmé avec l'application TPM, tel que présenté plus haut au paragraphe « Architecture » et configuré conformément au guide de personnalisation (cf. [GUIDES]). Le composant a été testé en mode opérationnel qui est le mode dans lequel il est livré à l'utilisateur, conformément au profil de protection [ANSSI-CC-PP-2015/07].

2. L'évaluation

2.1. Référentiels d'évaluation

L'évaluation a été menée conformément aux **Critères Communs version 3.1 révision 4** [CC], et à la méthodologie d'évaluation définie dans le manuel CEM [CEM].

Pour les composants d'assurance qui ne sont pas couverts par le manuel [CEM], des méthodes propres au centre d'évaluation et validées par l'ANSSI ont été utilisées.

Pour répondre aux spécificités des cartes à puce, les guides [JIWG IC] et [JIWG AP] ont été appliqués. Ainsi, le niveau AVA_VAN a été déterminé en suivant l'échelle de cotation du guide [JIWG AP]. Pour mémoire, cette échelle de cotation est plus exigeante que celle définie par défaut dans la méthode standard [CC], utilisée pour les autres catégories de produits (produits logiciels par exemple).

2.2. Travaux d'évaluation

L'évaluation s'appuie sur les résultats d'évaluation du produit « TPM 2.0 Hardware version FB5C85D, Firmware version 1.3.0.1 » certifié le 22 juillet 2016 sous la référence [CER-2016/15].

Le rapport technique d'évaluation [RTE], remis à l'ANSSI le 13 juillet 2017, détaille les travaux menés par le centre d'évaluation et atteste que toutes les tâches d'évaluation sont à « **réussite** ».

2.3. Cotation des mécanismes cryptographiques selon les référentiels techniques de l'ANSSI

La cotation des mécanismes cryptographiques selon le référentiel technique de l'ANSSI [REF], n'a pas été réalisée. Néanmoins, l'évaluation n'a pas mis en évidence de vulnérabilité de conception et de construction pour le niveau AVA_VAN.4 visé.

2.4. Analyse du générateur d'aléas

Pour le niveau AVA_VAN.4 visé, l'évaluation n'a pas mis en évidence de vulnérabilités exploitables du générateur d'aléas.

3. La certification

3.1. Conclusion

L'évaluation a été conduite conformément aux règles et normes en vigueur, avec la compétence et l'impartialité requises pour un centre d'évaluation agréé. L'ensemble des travaux d'évaluation réalisés permet la délivrance d'un certificat conformément au décret 2002-535.

Ce certificat atteste que le produit « NPCT6xx TPM 2.0, Hardware version FB5C85D and FB5C85E, Firmware version 1.3.0.1, 1.3.1.0 and 1.3.2.8 » soumis à l'évaluation répond aux caractéristiques de sécurité spécifiées dans sa cible de sécurité [ST] pour le niveau d'évaluation EAL 4 augmenté des composants ALC_DVS.2, ALC_FLR.1 et AVA_VAN.4.

3.2. Restrictions d'usage

Ce certificat porte sur le produit spécifié au chapitre 1 du présent rapport de certification.

L'utilisateur du produit certifié devra s'assurer du respect des objectifs de sécurité sur l'environnement d'exploitation, tels que spécifiés dans la cible de sécurité [ST], et suivre les recommandations se trouvant dans les guides fournis [GUIDES].
Plus spécifiquement, les recommandations suivantes doivent être suivies :

- la taille minimale des clés RSA doit être d'au moins 2048 bits ;
- la fonction de *hash* SHA-1 ne doit pas être utilisée pour des applications de sécurité.

3.3. Reconnaissance du certificat

3.3.1. Reconnaissance européenne (SOG-IS)

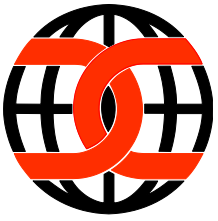
Ce certificat est émis dans les conditions de l'accord du SOG-IS [SOG-IS].

L'accord de reconnaissance européen du SOG-IS de 2010 permet la reconnaissance, par les pays signataires de l'accord[1], des certificats ITSEC et Critères Communs. La reconnaissance européenne s'applique, pour les cartes à puces et les dispositifs similaires, jusqu'au niveau ITSEC E6 Elevé et CC EAL7 lorsque les dépendances CC sont satisfaites. Les certificats reconnus dans le cadre de cet accord sont émis avec la marque suivante :

3.3.2. Reconnaissance internationale critères communs (CCRA)

Ce certificat est émis dans les conditions de l'accord du CCRA [CC RA].

L'accord « Common Criteria Recognition Arrangement » permet la reconnaissance, par les pays signataires[2], des certificats Critères Communs.
La reconnaissance s'applique jusqu'aux composants d'assurance du niveau CC EAL2 ainsi qu'à la famille ALC_FLR.
Les certificats reconnus dans le cadre de cet accord sont émis avec la marque suivante :



[1] La liste des pays signataires de l'accord SOG-IS est disponible sur le site web de l'accord : www.sogis.org.
[2] La liste des pays signataires de l'accord CCRA est disponible sur le site web de l'accord : www.commoncriteriaportal.org.

Annexe 1. Niveau d'évaluation du produit

Classe	Famille	Composants par niveau d'assurance							Niveau d'assurance retenu pour le produit	
		EAL 1	EAL 2	EAL 3	EAL 4	EAL 5	EAL 6	EAL 7	EAL 4+	Intitulé du composant
ADV Développement	ADV_ARC		**1**	1	1	1	1	1	**1**	Security architecture description
	ADV_FSP	**1**	**2**	**3**	**4**	**5**	5	**6**	**4**	Complete functional specification
	ADV_IMP				**1**	1	**2**	2	**1**	Implementation representation of TSF
	ADV_INT					**2**	**3**	3		
	ADV_SPM						**1**	1		
	ADV_TDS		**1**	**2**	**3**	**4**	**5**	**6**	**3**	Basic modular design
AGD Guides d'utilisation	AGD_OPE	**1**	1	1	1	1	1	1	**1**	Operational user guidance
	AGD_PRE	**1**	1	1	1	1	1	1	**1**	Preparative procedures
ALC Support au cycle de vie	ALC_CMC	**1**	**2**	**3**	**4**	4	**5**	5	**4**	Production support, acceptance procedures and automation
	ALC_CMS	**1**	**2**	**3**	**4**	**5**	5	5	**4**	Problem tracking CM coverage
	ALC_DEL		**1**	1	1	1	1	1	**1**	Delivery procedures
	ALC_DVS			**1**	1	1	2	**2**	**2**	Sufficiency of security measures
	ALC_FLR								**1**	Basic Flaw Remediation
	ALC_LCD			**1**	1	1	1	**2**	**1**	Developer defined life-cycle model
	ALC_TAT				**1**	**2**	**3**	3	**1**	Well-defined development tools
ASE Evaluation de la cible de sécurité	ASE_CCL	**1**	1	1	1	1	1	1	**1**	Conformance claims
	ASE_ECD	**1**	1	1	1	1	1	1	**1**	Extended components definition
	ASE_INT	**1**	1	1	1	1	1	1	**1**	ST introduction
	ASE_OBJ	**1**	**2**	2	2	2	2	2	**2**	Security objectives
	ASE_REQ	**1**	**2**	2	2	2	2	2	**2**	Derived security requirements
	ASE_SPD		**1**	1	1	1	1	1	**1**	Security problem definition
	ASE_TSS	**1**	1	1	1	1	1	1	**1**	TOE summary specification
ATE Tests	ATE_COV		**1**	**2**	2	2	**3**	3	**2**	Analysis of coverage
	ATE_DPT			**1**	1	**3**	3	**4**	**1**	Testing: basic design
	ATE_FUN		**1**	1	1	1	**2**	2	**1**	Functional testing
	ATE_IND	**1**	**2**	2	2	2	2	**3**	**2**	Independent testing: sample
AVA Estimation des vulnérabilités	AVA_VAN	**1**	**2**	2	**3**	**4**	**5**	5	**4**	Moderate vulnerability analysis

Annexe 2. Références documentaires du produit évalué

[ST]	Cible de sécurité de référence pour l'évaluation : - Security Target NPCT6xx TPM 2.0 (Hardware FB5C85D/FB5C85E, Firmware 1.3.0.1, 1.3.1.0, 1.3.2.8), Version 1.07, May 2017, Nuvoton Technology. Pour les besoins de publication, la cible de sécurité suivante a été fournie et validée dans le cadre de cette évaluation : - Public Security Target NPCT6xx TPM 2.0 (Hardware FB5C85D/ FB5C85E, Firmware 1.3.0.1, 1.3.1.0, 1.3.2.8), Version 1.07, May 2017, Nuvoton Technology.
[RTE]	Rapport technique d'évaluation : - Evaluation Technical Report TPM2.0 Project, reference NPCT6_ETR_v1.0, version 1.0, 13th July 2017, Serma Safety & Security.
[CONF]	Liste de configuration du produit : - TPM2.0_NPCT6xx_IC_ALC_CMS, version 0.6.5, February 2017, Nuvoton Technology ; - ALC_Doc_Report TPM2.0, version3.7, Nuvoton Technology.
[GUIDES]	- NPCT65x Trusted Platform Module Version 2.0 (TPM2.0), Revision 1.5, January 2017, Nuvoton Technology ; - NPCT65x TPM 2.0 Programmer's Guide, Revision 1.1, July 2016, Nuvoton Technology ; - NPCT6xx User Product Information, Revision 4.8, January 2017, Nuvoton Technology ; - NPCT6xx Board Design Guide, Revision 1.4, May 2015, Nuvoton Technology ; - NPCT620/622/650/652 Reference Schematics, Revision 1.6, May 2015, Nuvoton Technology ; - NPCT65xxxxA TPM2.0 Guidance Document, Revision 1.3, June 2016, Nuvoton Technology.
[CER-2016/15]	Rapport de certification ANSSI-CC-2016/15 « TPM 2.0**,** Hardware version FB5C85D, Firmware version 1.3.0.1 » émis le 22 juillet 2016, ANSSI.
[ANSSI-CC-PP-2015/07]	Protection Profile - PC Client Specific Trusted Platform Module, Family 2.0, Level 0, Revision v1.16, Version 1.0. Certifié par l'ANSSI (*Agence Nationale de la Sécurité des Systèmes d'Information*) le 6 mai 2015 sous la référence ANSSI-CC-PP-2015/07.

Annexe 3. Références liées à la certification

Décret 2002-535 du 18 avril 2002 modifié relatif à l'évaluation et à la certification de la sécurité offerte par les produits et les systèmes des technologies de l'information.	
[CER/P/01]	Procédure CER/P/01 Certification de la sécurité offerte par les produits et les systèmes des technologies de l'information, ANSSI.
[CC]	Common Criteria for Information Technology Security Evaluation : Part 1: Introduction and general model, septembre 2012, version 3.1, révision 4, référence CCMB-2012-09-001; Part 2: Security functional components, Septembre 2012, version 3.1, révision 4, référence CCMB-2012-09-002; Part 3: Security assurance components, septembre 2012, version 3.1, révision 4, référence CCMB-2012-09-003.
[CEM]	Common Methodology for Information Technology Security Evaluation : Evaluation Methodology, septembre 2012, version 3.1, révision 4, référence CCMB-2012-09-004.
[JIWG IC] *	Mandatory Technical Document - The Application of CC to Integrated Circuits, version 3.0, février 2009.
[JIWG AP] *	Mandatory Technical Document - Application of attack potential to smartcards, version 2.9, janvier 2013.
[CC RA]	Arrangement on the Recognition of Common Criteria Certificates in the field of Information Technology Security, 2 juillet 2014.
[SOG-IS]	« Mutual Recognition Agreement of Information Technology Security Evaluation Certificates », version 3.0, 8 janvier 2010, Management Committee.
[REF]	Mécanismes cryptographiques – Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques, version 1.20 du 26 janvier 2010 annexée au Référentiel général de sécurité, voir http://www.ssi.gouv.fr.
[NOTE6.2]	Note d'application n°6 « Exigences de sécurité pour un chargement de code en phase d'utilisation », version 2.0, 23 janvier 2015, ANSSI.

*Document du SOG-IS ; dans le cadre de l'accord de reconnaissance du CCRA, le document support du CCRA équivalent s'applique.